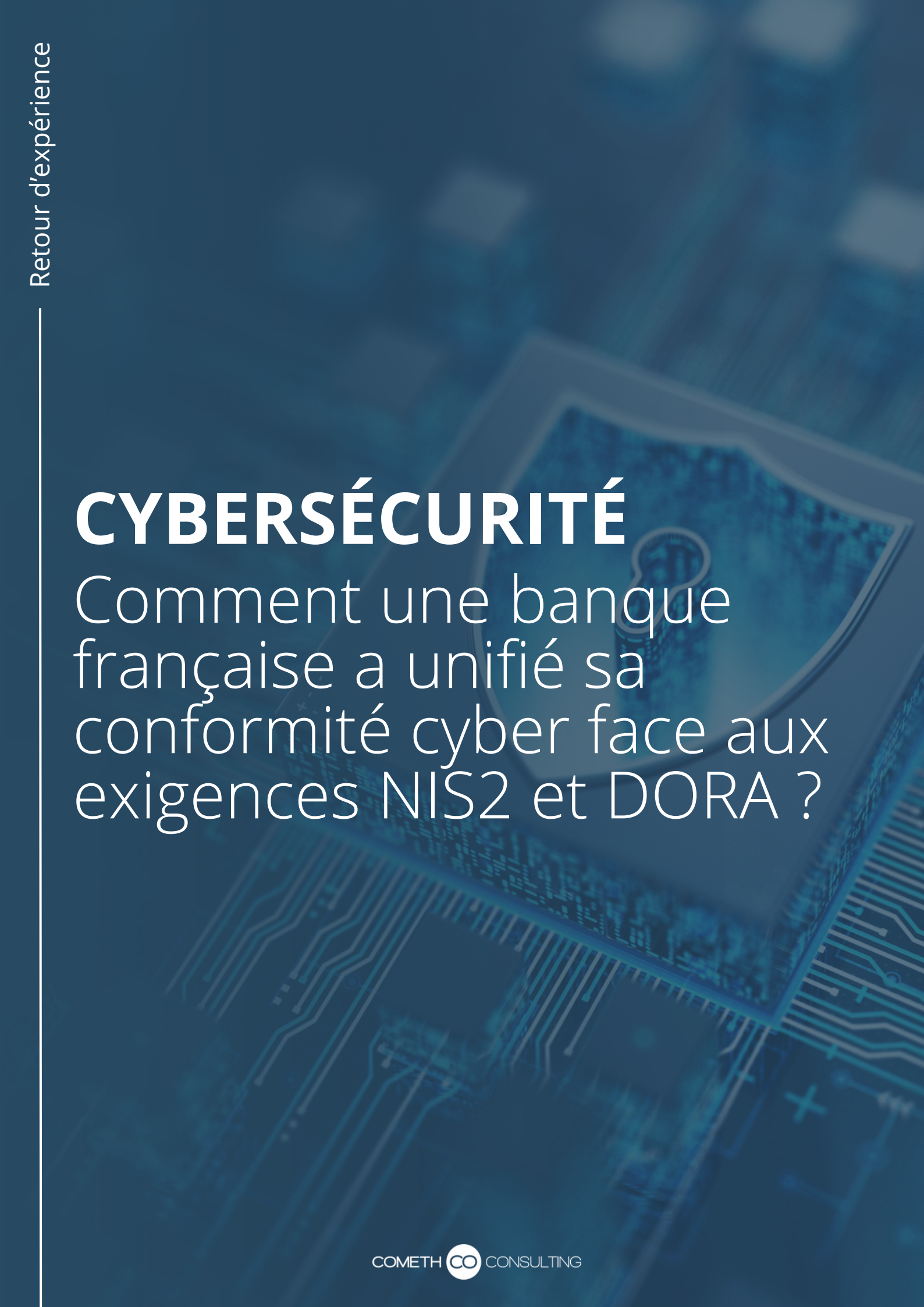
Retour d'expérience

CYBERSÉCURITÉ

Comment une banque française a unifié sa conformité cyber face aux exigences NIS2 et DORA ?



COMETH CO CONSULTING

Pour beaucoup d'institutions financières, l'audit cyber est souvent vécu comme une pression réglementaire de plus dans un agenda déjà surchargé.

Pourtant, face à l'explosion des menaces, c'est un outil formidable pour détecter les failles techniques, optimiser l'organisation et cibler les besoins en formation.

Découvrez comment nous accompagnons un grand acteur bancaire français depuis 2023 dans son programme international.

L'enjeu ? Industrialiser et capitaliser sur ses audits cyber pour sécuriser durablement des milliers d'applications à travers plus de 30 pays, grâce à une démarche robuste et homogène.

UN PROGRAMME DE CONFORMITÉ À GRANDE ÉCHELLE

Face à une pression réglementaire sans précédent (NIS2, PASSI-LPM, PCI-DSS, ISO 27001…), **la Direction Générale et la Direction Cyber de ce grand groupe ont fait un choix stratégique fort : casser les silos et industrialiser les évaluations de bout en bout.**

La clé du succès ?

Un déploiement progressif et structuré pour sécuriser un périmètre hautement critique, le tout sans jamais perturber le quotidien opérationnel des équipes métiers.

DES DÉFIS MULTIPLES POUR UNE TRANSFORMATION TRANSVERSALE

Ce projet s'inscrit comme un programme structurant à très forte visibilité interne. Mener à bien cette transition nécessitait de relever cinq défis simultanés :

Cartographie du SI (Priorisation des actifs)

Identifier et hiérarchiser les actifs critiques au sein d'un patrimoine applicatif immense pour focaliser les efforts

Harmonisation dans les entités

Unifier et standardiser les pratiques d'audit entre les DSI locales et les multiples filiales étrangères

Conformité et plans de remédiation

Piloter et planifier de manière rigoureuse les plans de remédiations post-audit pour s'assurer de la correction effective des failles

Gestion des tiers (TPRM)

Étendre le niveau d'exigence et le dispositif d'audit aux prestataires externes et partenaires stratégiques

Conduite du changement

Sensibiliser et embarquer les équipes métier afin qu'elles intègrent la cybersécurité comme un réflexe au quotidien et non comme un frein

NOTRE RÔLE : SÉCURISER, CHALLENGER ET COORDONNER LA TOUR DE CONTRÔLE CYBER

Dans le cadre de ce programme d'envergure, Cometh Consulting est intervenu en tant qu'AMOA Cybersécurité, jouant un rôle central de tour de contrôle entre l'audit interne, le SOC, les équipes métiers et la Direction Générale. Notre positionnement a permis d'assurer un relais opérationnel fluide tout en challengeant l'avancement des chantiers pour garantir l'alignement constant avec les exigences de conformité.

Notre intervention s'est articulée de bout en bout autour de 4 phases clés :

PHASE DE CADRAGE

Définition de la stratégie globale, priorisation des applications critiques et formalisation des référentiels d’audit.

PHASE D'AUDIT

Coordination des campagnes d'évaluation à l'échelle internationale et harmonisation des méthodes de collecte au sein des entités.

PHASE DE REMÉDIATION

Structuration et suivi des plans de correction des vulnérabilités, en lien étroit avec les DSI locales et les managers.

PHASE DE RUN

Stabilisation des processus industrialisés, transfert de compétences et sécurisation du modèle opérationnel pour les vagues d'audits futures.

DES BÉNÉFICES QUI DÉPASSENT LE SIMPLE EXERCICE DE CONFORMITÉ

L'adoption d'un socle d'audit unifié et la collaboration étroite entre les différentes lignes de défense ont permis de tirer des bénéfices tangibles et mesurables :

Mitigation des risques — Une diminution de 45 % des vulnérabilités critiques non traitées constatée en l'espace de 12 mois.

Force collaborative — Une collaboration étroite avec les managers pour aligner l'ensemble des systèmes sur les objectifs de la nouvelle régulation européenne DORA.

Autonomie renforcée — Une montée en compétences et une plus grande responsabilisation des DSI locales face à leurs enjeux de sécurité spécifiques.

Standardisation internationale — Un écosystème de pratiques cyber rationalisé et partagé entre le siège et ses filiales.

Culture de la preuve — Une amélioration significative de la transparence interne face aux régulateurs et auditeurs (internes et externes) de l'Inspection Générale (IG).

LES ENSEIGNEMENTS CLÉS DU PROJET

1 LE SPONSORSHIP EST LE MOTEUR

Une gouvernance engagée au plus haut niveau (Direction Générale) et un sponsorship fort sont absolument indispensables pour imposer des standards cyber internationaux.

2 L'IMPLICATION DES MÉTIERS EST CRITIQUE

La sécurité ne doit pas rester un sujet de spécialistes. L'implication forte des directions métiers en amont conditionne la réussite de la remédiation.

3 LE PILOTAGE GROUPE / FILIALES DOIT ÊTRE CO-CONSTRUIT

Mettre en place des mécanismes de pilotage équilibrés permet de respecter les spécificités locales tout en maintenant le niveau d'exigence du Groupe.

4 UN SOCLE COMMUN ÉVITE LES BLOCAGES

La définition claire d'un socle commun de conformité doit être traitée le plus en amont possible pour harmoniser la trajectoire de sécurité.

5 LA CULTURE DE LA PREUVE ENGENDRE LA RIGUEUR

L'amélioration continue de la collecte de données est essentielle pour passer d'une logique de conformité théorique à une gouvernance fondée sur les preuves, ancrée dans le réel.

COMETH CONSULTING

Cometh Consulting est un cabinet de conseil indépendant fondé en 2010. Fort de plus de 15 ans d'expérience, nous accompagnons les acteurs de la banque et de l'assurance dans la réussite de leurs missions stratégiques et opérationnelles.
Notre expertise s'articule autour de quatre piliers majeurs :

- Cybersécurité & Gestion des risques (DORA, NIS2, PCI-DSS, ISO 27001)
- Conformité réglementaire
- Gouvernance de la donnée
- Transformation digitale

En tant que tour de contrôle AMOA, nous coconstruisons votre stratégie cyber pour cartographier vos actifs critiques, fiabiliser vos indicateurs de sécurité et industrialiser vos dispositifs d'audit de bout en bout.
Notre ambition : Accompagner la montée en maturité de vos équipes pour transformer les contraintes de conformité en un véritable levier de résilience durable.

EN SAVOIR PLUS